A guide to "reasonable lines of enquiry" and Communications Evidence

JULY 2018

CPS

Contents

Introduction

This document sets out guidance as to the approach that ought to be adopted by prosecutors, in accordance with their duties under the Criminal Procedure and Investigations Act 1996 ('CPIA'), and the relevant Codes issued under and in pursuance to that Act. In particular, it seeks to address the issues that arise in the context of allegations where the accused and the complainant are known to each other, and where the smart phone or similar digital devices of the complainant or others may contain communication that may be relevant to the case, and would fall to be disclosed.

This guidance should be read in conjunction with the Disclosure – Guidance on Communication Evidence (published 26 January 2018). A thinking approach is crucial; every case is and must be fact specific. Set out below are examples of how the application of the legal principles could be approached by prosecutors in practice.

Relevant principles of disclosure

1 Section 3(1)(a) of the CPIA provides a single test for disclosure and requires the prosecution to:

"… disclose to the accused any prosecution material which has not previously been disclosed to the accused and which might reasonably be considered capable of undermining the case for the prosecution against the accused or of assisting the case for the accused".

"Prosecution material" is defined in section 3(2) as material: (a) which is in the prosecutor's possession, and came into his possession in connection with the case for the prosecution against the accused; or (b) which has been inspected in connection with the case for the prosecution against the accused.

2 The Code of Practice issued under section 23(1), CPIA (in its March 2015 edition) identifies at part 3 general responsibilities relevant to this disclosure duty. In particular, paras.3.4-5 state:

"…In conducting an investigation, the investigator should pursue all reasonable lines of inquiry, whether these point towards or away from the suspect. What is reasonable in each case will depend on the particular circumstances. For example, where material is held on computer, it is a matter for the investigator to decide which material on the computer it is reasonable to inquire into, and in what manner." Relevant material is defined (at para.2.1) as: "…it has some bearing on any offence under investigation or any person being investigated, or on the surrounding circumstances of the case, unless it is incapable of having any impact on the case".

3 Part 5 of the Code addresses the obligation to retain such material at least until a charging decision, and, following charge, until the conclusion of proceedings. At para.5.1 it states:

"Material may be photographed, video-recorded, captured digitally or otherwise retained in the form of a copy rather than the original at any time, if the original is perishable; the original was supplied to the investigator rather than generated by him and is to be returned to its owner; or the retention of a copy rather than the original is reasonable in all the circumstances." Para.5.3 goes on to indicate: "If the officer in charge of an investigation becomes aware as a result of developments in the case that material previously examined but not retained (because it was not thought to be relevant) may now be relevant to the investigation, he should, wherever practicable, take steps to obtain it or ensure that it is retained for further inspection or for production in court if required."

4 The Attorney General's Guidelines on Disclosure of Unused Material in Criminal Proceedings issued in 2013 address in the Annex to the document how these obligations are to be applied where the material in question is of a size or nature that makes its examination impractical. At para.3 of the Annex it says:

"(i) Investigating and prosecuting agencies, especially in large and complex cases, will apply their respective case management and disclosure strategies and policies and be transparent with the defence and the courts about how the prosecution has approached complying with its disclosure obligations in the context of the individual case; and, (ii) The defence will be expected to play their part in defining the real issues in the case. In this context, the defence will be invited to participate in defining the scope of the reasonable searches that may be made of digitally stored material by the investigator to identify material that might reasonably be expected to undermine the prosecution case or assist the defence."

5 More recently, in R [2015] EWCA Crim 1941; [2016] 1 Cr. App. R. 20, the Court of Appeal issued a practice note in which Sir Brian Leveson PQBD summarised the relevant principles and said (at para.34) :

"…To fulfil its duty under s.3 , the prosecution must adopt a considered and appropriately resourced approach to giving initial disclosure. Such an approach must extend to and include the overall disclosure strategy, selection of software tools, identifying and isolating material that is subject to legal professional privilege (LPP) and proposing search terms to be applied. The prosecution must explain what it is doing and what it will not be doing at this stage, ideally in the form of a "Disclosure Management Document". This document, as recommended by the Review and the Protocol, is intended to clarify the prosecution's approach to disclosure (for example, which search terms have been used and why) and to identify and narrow the issues in dispute. By explaining what the prosecution is, and is not, doing, early engagement from the defence would be prompted"

The examination of digital media devices

6 Mobile devices are not standard and the ability of digital forensic services to access data varies between manufacturers, models, operating systems and even versions of the same model of a device and may also change over time.

7 It is not possible to obtain and examine every artefact or item of digital evidence from a device for analysis in every situation – there are constraints to the extent and depth of an examination in the circumstances of each case. It is critical that the investigator and prosecutor are aware of the opportunities presented by a device and the limitations and boundaries of an examination; including the implications of utilising one examination methodology over another if further work is required in the future.

Although capabilities vary across England and Wales, there are essentially 3 levels of data extraction and examination of mobile devices offered by the digital forensic services, namely:

i) **Level 1** – Configured Logical Extraction - Digital Forensics Kiosks,
ii) **Level 2** – Logical & Physical Extraction - Digital Forensics Hubs or Laboratories or Forensic Service Providers, and
iii) **Level 3** – Specialist Extractions & Examinations - Central Digital Forensics Laboratories or Forensic Service Providers.

8 Terms such as “Full” extractions or downloads should be avoided as they can easily lead to assumptions and misinterpretation of the actual agreed method(s) of examination.

9 A Digital Forensics Kiosk or Self Service equipment is officer operated equipment based within operational police premises. These officers are usually non practitioners, trained and competent to follow a preconfigured workflow on the equipment. These data extractions are sometimes referred to by officers by referring to the vendor of the equipment and extraction software e.g. “XRY, Cellebrite or Aceso downloads”.

10 **Level 1 mobile device examination** provides a “logical” extraction. A “logical” extraction provides the live data that is readily available on device, probably all of the data you could see if you were able to turn on the device and browse through it. A logical extraction will extract the live data that is supported by the extraction software. This could vary by handset, operating system and types of applications. It may not extract all of the data present and will not usually extract deleted material.

11 **Level 2 mobile device examination** can be either a “logical” extraction using selected tools in a laboratory environment to report that data or a “physical” extraction, which recovers a bit for bit copy of the data held on the memory chip of the device. “Physical” downloads can extract deleted data, although again capabilities vary depending on the nature of the device, operating system, types of applications and whether they are supported by the extraction software.

12 **Level 3 mobile device examinations** are usually expert and bespoke methods to tackle complex issues or damaged devices. Examples include specialist evaluation and interpretation of digital data or Level 1, 2, or 3 data extraction.

Application of the principles

13 The examination of mobile devices belonging to the complainant is not a requirement as a matter of course in every case. There will be cases where there is no requirement for the police to take the media devices of a complainant or others at all, and thus no requirement for even a level 1 examination to be undertaken. Examples of this would include sexual offences committed opportunistically against strangers, or historic allegations where there is considered to be no prospect that the complainant’s phone will retain any material relevant to the period in which the conduct is said to have occurred and/or the complainant through age or other circumstances did not have access to a phone at that time.

14 There are equally cases where a level 1 examination is sufficient as a first step. Examples include cases where the parties are known to each other, particularly for a short period, but where there is no particular reason to consider that their communications will be of importance but there is the possibility that they will be of relevance. In such circumstances, the use of a level 1 examination is a reasonable first examination stage, always with the caveat that if either that level 1 examination reveals the need for a more detailed examination, or other material generated by the investigation, for example from an account in interview or via a defence statement from the accused, requires a deeper examination of the content of a device.

15 It would be prudent to retain a complainant’s phone until there has been an opportunity to provide the accused with an opportunity to comment on the allegation, either through an interview or through liaison with defence representatives. This precaution itself will be fact sensitive, in that there may be cases where the delay to the return of a phone to a complainant

would be disproportionate, but that consideration must be judged cautiously, with the benefit of the doubt resolved in favour of retaining the phone until an informed decision as to the level of necessary phone examination can be made.

16 There will also be cases where the requirement from the outset is to undertake a level 2 or level 3 examination. These are likely to be required in every case where the offence is committed using electronic means, for example sexual communication with a child or possession of indecent images of children. This will also be the case where, beyond the issue of consent being raised at all by either complainant or accused, the credibility of the complaint or reliability of the complainant is put in issue from the outset and in circumstances that make a detailed examination of the complainant's phone necessary. This is a case by case assessment, but examples would include cases where the account of the complainant or an account provided by an accused either in interview or to others at a stage identifies a need to examine the past history and content of contact between the complainant and accused, or the complainant and an identified third party, and where there it is thought likely to be material of a kind that a level 1 search may not identify relevant to such issues.

Analysis of the material

17 In examining the contents of a mobile device download, the investigator may set parameters relating to timeframes that are proportionate to the facts, for example between the date the complainant and suspect met to a month after the suspect's arrest. If there are messages that are potentially undermining / assisting at either end of the window of time searched, then the search should be extended further.

18 As with all communication evidence, the prosecution must be able to explain to the defence and the court what we are doing as well as, importantly, what we will not be doing. Transparency of the approach that has been taken in every case is of paramount importance. The prosecution should encourage early dialogue with the defence as to what has been considered reasonable. Below is an example of how this might be recorded in the Disclosure Record Sheet (DRS) and Disclosure Management Document (DMD);

The following mobile devices were seized and have been examined and download reports prepared;

Exhibit Reference	Description of telephone	Telephone obtained from	Telephone number	Download report reference
ABC/1	iPhone x	suspect	XXXXX XXXXXX	DEF/1
ABC/2	Nokia x	complainant	XXXXX XXXXXX	DEF/2

The contents of the download in respect of the telephone ABC/1 between 1/1/2017 and 1/7/2017 have been examined for the following;

Level 2 Mobile Device Examination:

(i) Logical Capture and Preservation of case defined and verified data (from Handset, Tablet, (U)SIM or Memory Card) using selected tool(s) in a laboratory environment to report that data.
(ii) Physical Capture and Preservation of data (from Handset, Tablet or Memory Card) using selected tool(s) in a laboratory environment to report defined data types.

- Text messages
- Emails
- Calls
- Social media – including Facebook, Instagram, WhatsApp etc

The timeframe selected is considered to be a proportionate and reasonable line of enquiry, and represents [e.g. the date that the complainant first met the suspect to a month after the suspect's arrest]

The device has been examined for communications between the complainant and the suspect that relate to [insert parameters of the search that has been made e.g. communications about the offence or appear relevant to an issue in the case such as previous sexual behaviour between them, issues raised in interview, material that points away from the offence].

19 What represents a reasonable line of enquiry is an investigative matter for the police and whilst the prosecution will do what they can to assist in identifying potential further enquiries, that ought not to be taken by the police as definitive or exhaustive.